

Dual quantum information splitting with degenerate graph states

Akshata Shenoy H,^{1,*} R. Srikanth,^{2,3,†} and T. Srinivas¹

¹*Applied Photonics Lab, ECE Dept., IISc, Bangalore, India*

²*Poornaprajna Institute of Scientific Research, Bengaluru, India*

³*Raman Research Institute, Bengaluru, India.*

We propose a protocol for secret sharing, called dual quantum information splitting (DQIS), that reverses the roles of state and channel in standard quantum information splitting. In this method, a secret is shared via teleportation of a fiducial input state over an entangled state that encodes the secret in a graph state basis. By performing a test of violation of a Bell inequality on the encoded state, the legitimate parties determine if the violation is sufficiently high to permit distilling secret bits. Thus, the code space must be maximally and exclusively nonlocal. To this end, we propose two ways to obtain code words that are degenerate with respect to a Bell operator. The security of DQIS comes from monogamy of nonlocal correlations, which we illustrate by means of a simple single-qubit attack model. The nonlocal basis of security of our protocol makes it suitable for security in general monogamous theories and in the more stringent, device-independent cryptographic scenario.

I. INTRODUCTION

Quantum entanglement enables tasks in communication and cryptography not possible in the classical world, e.g., quantum teleportation [1], dense coding and unconditionally secure key distribution [2]. Experimental breakthroughs have enabled practical creation and manipulation of entanglement [3], an achievement duly recognized by the 2012 Nobel prizes in physics. Several teleportation-based protocols with multi-particle channels have been proposed [4–12]. In particular, entanglement can be used for quantum secret sharing (QSS), the quantum version of classical secret sharing [13]. QSS involves a secret dealer splitting information, representing the secret quantum state $|\Psi\rangle$, among a number of agents, such that only authorized subsets of them can reconstruct the secret.

A protocol for splitting quantum information, and teleporting it to more than one party over an entangled channel, such that a subset of agents sharing the entanglement, is able to reconstruct the information, was first proposed in Ref. [14], further studied by various authors [15–19], and also implemented experimentally [20–22] (the last employing only sequential measurements on a single qubit). We will refer to such teleportation-based QSS as quantum information splitting (QIS). Both QSS and QIS can be used to share both quantum and classical secrets.

An important resource of entanglement are *graph states* that are useful in quantum error correction [23], one-way quantum computing [24] and cryptography [10, 25–27]. They have been studied extensively theoretically, and been realized experimentally recently [28, 29].

Given a graph $G = (V, E)$ defined by the set V of n vertices, and set E of edges, we denote by $\mathcal{N}(j)$, the set of vertices with which vertex j is connected by an edge

(the neighborhood). Corresponding to each vertex j , one can associate a stabilizer operator:

$$g_j = X_j \bigotimes_{k \in \mathcal{N}(j)} Z_k, \quad (1)$$

where Z_k and X_k , along with Y_k , denote Pauli matrices acting on qubit k . We define the graph state basis by the 2^n common eigenstates $|G_{\mathbf{x}}\rangle \equiv |G_{x_1 x_2 \dots x_n}\rangle = \bigotimes_j (Z_j)^{x_j} |G_{000\dots 0}\rangle$, with $(x_j \in \{0, 1\})$ of the n commuting operators g_j , where $g_j |G_{x_1 x_2 \dots x_n}\rangle = (-1)^{x_j} |G_{x_1 x_2 \dots x_n}\rangle$. In particular, the canonical n -qubit graph state $|G\rangle \equiv |G_{00\dots 0}\rangle$ is characterized by n independent perfect correlations of the form

$$g_j |G\rangle = |G\rangle. \quad (2)$$

The set of all 2^n products (h_k) of the g_j 's forms the stabilizer group \mathcal{S} . It follows from Eq. (2) that $h_j |G\rangle = |G\rangle$ for all $h_j \in \mathcal{S}$. Graph states are robust against decoherence [30], which enhances their practical value.

An alternate equivalent definition of graph states, based on their generation via an Ising type of interaction, is as follows:

$$|G\rangle = \Pi_{(j,k) \in E} \mathcal{C}_Z^{\{j,k\}} |+\rangle, \quad (3)$$

where \mathcal{C}_Z is the controlled-phase gate. Here we use the usual notation $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$, $X|\pm\rangle = \pm|\pm\rangle$.

A special class of graph states are the linear cluster states, which correspond to a linear graph. An n -qubit cluster state is given by:

$$|\phi_N\rangle = \frac{1}{2^{n/2}} \bigotimes_j (|0\rangle + |1\rangle_j Z_{j+1}), \quad (4)$$

with $Z_{n+1} \equiv 1$. For example,

$$|\phi_4\rangle = \frac{1}{2} (|+0+0\rangle + |+0-1\rangle + |-1-0\rangle + |-1+1\rangle), \quad (5)$$

where we use the notation $|+0+0\rangle = |+\rangle|0\rangle|+\rangle|0\rangle$, etc. It should be noted that different graphs may lead to the

*Electronic address: akshata@ece.iisc.ernet.in

†Electronic address: srik@poornaprajna.org

same graph state modulo local transformations. For example, a star graph over n vertices leads to the same state irrespective of vertex it is rooted in. The principal graph transformation that leaves the entanglement property of a graph state invariant is *local complementation* [31].

As highly entangled states, graph states show nonlocal correlations [31–41] that contradict the assumption of local-realism, as demonstrated by their violation of Bell-type inequalities [42, 43]. This is of cryptographic interest because there is a close connection between security and the violation of a Bell-type inequality [44–46]. This connection assumes further importance in the device independent (DI) scenario, where eavesdropper Eve is allowed to conceal additional dimensions in the devices of legitimate parties, that empower a side channel which leaks basis and output information to Eve.

The remaining article is structured as follows. In Section II, we introduce a twist to the QIS idea, which we term *dual* QIS, or DQIS, wherein a fixed fiducial state of an ancilla is teleported over an entangled state that encodes the secret and satisfies certain conditions of teleportation. In Section III, we study the nonlocality of the DQIS code space, pointing out two ways of constructing Bell-type inequalities suitable to witness its nonlocality. In Section IV, we discuss the security of the DQIS based on the violation of the Bell-type inequalities, in particular, touching upon the device-independent scenario [47, 48]. A simple single-qubit eavesdropping attack on DQIS based on a 5-qubit 1-bit error correcting code is given, to illustrate how Eve’s entangling action can be detected because of monogamy of quantum nonlocal correlations. Finally, we conclude in Section V.

II. DUAL QUANTUM INFORMATION SPLITTING

In standard QIS, one teleports an unknown state $|\Psi\rangle$ (the secret) over a teleportation channel, which is a suitably entangled state. By contrast, in DQIS, we teleport a *fiducial* state, $|0\rangle$ by convention, across an entangled state $|\Psi_L\rangle$ that encodes $|\Psi\rangle$, such that the end result of the teleportation is the recovery of $|\Psi\rangle$.

DQIS can be useful in situations where the qudit secret $|\Psi\rangle$ is priorly known to the dealer Alice, before the distribution of the entangled particles to the agents, and furthermore it is unsafe for Alice to store $|\Psi\rangle$ indefinitely in her station. This may be the case in situations where Alice has bounded quantum memory, and cannot stock secrets (in addition to her entangled particles), but is able to prepare a fixed state when transmission is needed. Alice classically encrypts $|\Psi\rangle$ using one of d^2 operations [18], and transmits it to a distributor Dolly, who encodes it into an entangled state, which is transmitted to all relevant parties.

For example, the classical encryption of a qubit requires the equi-probable application of the 4 four Pauli operations, which transforms a qubit in an arbitrary state

into a maximally mixed state. Alice must divulge the two-bit (in general, $2 \log d$ bits) decyption information for recovery. Of course the dealer may also be the distributor.

The basic DQIS protocol works as follows:

1. Alice prepares the N copies of the d -dimensional secret $|\Psi\rangle = \sum_{j=1}^d \alpha_j |j\rangle$, classically encrypts each of them, and transmits them to Dolly, the distributor.
2. Dolly encodes each of them into an entangled state consisting of a superposition of suitable graph basis states. For example, state $|\Psi\rangle$ is encoded as:

$$|\Psi_L\rangle = \sum_{j=1}^d \alpha_j |G_j\rangle. \quad (6)$$

The $|G_j\rangle$ ’s are chosen so that they are suitable for QIS and satisfy an additional, teleportation condition discussed below.

3. Dolly transmits the qubits in her possession to the legitimate parties Alice, Bob, Charlie, Rex, et al. After their receipt has been acknowledged over an authenticated classical channel, she randomly selects $N - 1$ of the transmitted states, and announces their serial numbers.
4. The parties perform their local operations chosen randomly from a pre-agreed set, and communicate their classical outputs to Alice.
5. Alice performs a basis reconciliation where she determines if the measurements are appropriate to compute pre-agreed products (stabilizers h_j) of local Pauli operations on the particles. If the measurements correspond to none of the pre-agreed h_j ’s, they are discarded. Else, they are used to test the violation of a Bell-type inequality, which has the form:

$$\langle \mathcal{B} \rangle \equiv \sum_{j=1}^m \langle h_j \rangle \leq 2q - m, \quad (7)$$

where \mathcal{B} is the Bell operator and q ($\leq m$) is the largest number of the h_j ’s that assume a positive value (+1) if each particle is assumed to possess a definite value of X, Y, Z irrespective of the measurement setting on any other particle. A contradiction with *local-realism*, and hence a demonstration of quantum nonlocality, occurs when $q < m$.

The quantum bound on the l.h.s of Eq. (7) is the algebraically allowed maximum of m . Alice determines if the basis reconciled correlation data derived from the $N - 1$ states is compatible with distillable secrecy (by checking if they produce a sufficiently high violation of a Bell inequality).

6. If the inequality (7) is found to be violated sufficiently highly, Alice teleports the fiducial state $|0\rangle$, and signals the other agents to proceed to the next step: they perform standard teleportation measurements on their particles on the unmeasured state, and convey the resulting classical information to the recoverer, Rex.
7. Rex recovers the encrypted secret based on the classical communication from all other parties.
8. Alice gives Rex the classical decryption information, from which Rex recovers $|\Psi\rangle$.

The type of encoding in Eq. (6) must be such that Rex recovers $|\Psi\rangle$ even though Alice teleports $|0\rangle$. The conditions under which this works are discussed in the following Section II A. It might be thought that since the secret is encoded in the distributed entanglement, and the teleported state is publicly known, therefore the teleportation may be entirely eliminated. Still, the teleportation is needed so that the distributed state can be accessed via local operations and classical communication (LOCC) between the parties.

The issue of conditions under which the parties are able to perform a test of Bell inequality violation on the encoded state, is discussed in Section III. From an experimental perspective, implementing our protocol is not expected to be difficult in a set-up that realizes graph states, since the only additional requirement is creation of superposition of these states.

A. DQIS conditions for a qudit

We define a *teleportation configuration* \mathbf{C} as an arrangement of agents and their actions that fixes who the secret dealer (Alice) is, who the recoverer (Rex) is, etc., and what their local operations are. Two such basis states, which we denote $|G_0\rangle$ and $|G_1\rangle$, constitute a teleportationally *divergent* pair, if for a fiducial input state (taken here to be $|0\rangle$), Rex recovers $|j\rangle$ ($|\bar{j}\rangle$) when the channel is G_0 (G_1), for a given \mathbf{C} , and classical measurement outcome \mathbf{M} of all other parties.

More generally, consider a d -dimensional secret (a qudit state), and n -qubit graph basis states $|G_j\rangle$ ($j =$

$1, \dots, d$ where $d \leq 2^n$) associated with a graph $G(E, V)$. Letting:

$$|\psi_j\rangle_R = {}_{uA\xi}\langle v_k|0\rangle_u|G_j\rangle_{AR\xi}, \quad (8)$$

teleportation divergence entails that there exists a recovery operation $U_{\mathbf{C}, \mathbf{M}}^\dagger$ such that:

$$|\psi_j\rangle = U_{\mathbf{C}, \mathbf{M}}|j\rangle. \quad (9)$$

Here the labels u, A, R and ξ denote the ancilla, Alice, Rex and the remaining agents; $|v_k\rangle$ is a particular measurement outcome collectively obtained by all but Rex. The set of graph states that satisfy (8) and (9) for all $|v_k\rangle$ allowed under \mathbf{C} are said to be *teleportation divergent*.

Eq. (8) can be regarded as defining the map $\mathcal{T}_{\mathbf{C}, \mathbf{M}}$, for a given measurement configuration and conditioned on measurement outcomes \mathbf{M} . We have by virtue of quantum mechanical linearity, Eqs. (9) and (6)

$$\mathcal{T}_{\mathbf{C}, \mathbf{M}}(|\Psi_L\rangle) = U_{\mathbf{C}, \mathbf{M}} \left(\sum_j \alpha_j |j\rangle \right). \quad (10)$$

Thus, conditioned on the classical information \mathbf{M} , Rex recovers the secret $|\Psi\rangle$.

In the following two subsections, we illustrate DQIS of a qubit secret with a 4-qubit cluster state subspace, and the code space of a 5-qubit quantum error correcting (QEC) code. To conclude this subsection, we consider a simple example where DQIS fails for a particular choice of $|G_j\rangle$ and \mathbf{C} . These are taken to be graph basis states given by the GHZ class states

$$\begin{aligned} |G_{000}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \\ |G_{100}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \end{aligned} \quad (11)$$

We choose the configuration where Alice holds qubit 1 and measures the ancillary qubit and her entangled qubit in the Bell basis, Bob holds qubit 2 and measures in the X basis, and Charlie must recover the secret. One finds:

$$\begin{aligned} \alpha|0\rangle_C + \beta|1\rangle_C &\propto {}_{uA}\langle \Phi^+|_B\langle +|(\alpha|0\rangle_u + \beta|1\rangle_u)|G_{000}\rangle_{ABC}, \\ \alpha|0\rangle_C - \beta|1\rangle_C &\propto {}_{uA}\langle \Phi^+|_B\langle +|(\alpha|0\rangle_u + \beta|1\rangle_u)|G_{100}\rangle_{ABC}. \end{aligned} \quad (12)$$

As the l.h.s of Eqs. (12) are not mutually orthogonal, clearly there is no $U_{\mathbf{C}, \mathbf{M}}^\dagger$ such that the recovery condition (9) is satisfied. It follows that if Alice teleports the state $|0\rangle$ across the channel given by $|\Psi_L\rangle$ in Eq. (6) with

the code words given by Eq. (11), then under this configuration the state recovered is not the secret but simply $|0\rangle$.

B. Example: DQIS with cluster state space

Letting $d = 2$ in Eq. (6), we choose $|G_0\rangle$ to be $|\phi_{0000}\rangle \equiv |\phi_4\rangle$ in Eq. (5), and $|G_1\rangle \equiv |\phi_{0101}\rangle = Z_2 Z_4 |\phi_{0000}\rangle$, with fiducial input state being $|0\rangle$. Alice holds the input $|0\rangle$ and qubit 1, Bob qubits 2 and 3, and Rex qubit 4. The secret $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is encoded as:

$$|\Psi_L\rangle = \alpha|\phi_{0000}\rangle + \beta|\phi_{0101}\rangle, \quad (13)$$

where $|\alpha|^2 + |\beta|^2 = 1$. Alice measures in the Bell basis $\{|\Phi^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Psi^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)\}$, while

Bob in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, and Rex in the X basis. It may be verified that these $|G_j\rangle$'s satisfy the divergence conditions for the above configuration **C**. Alice's outcomes are tabulated in Table I, and Bob's outcomes corresponding to Alice's outcome $|\Phi^+\rangle$ in Table II. Based on Alice's 1 bit and Bob's 2 bit classical communication about their outcomes, Rex reconstructs $|\Psi\rangle$.

Alice's measurement	State obtained
$ \Phi^\pm\rangle$	$(\alpha + \beta)(0 + 0\rangle + 1 + 1\rangle) + (\alpha - \beta)(0 - 1\rangle + 1 - 0\rangle)$
$ \Psi^\pm\rangle$	$(\alpha + \beta)(0 + 0\rangle - 1 - 0\rangle) + (\alpha - \beta)(0 - 1\rangle - 1 + 1\rangle)$

TABLE I: 4-qubit cluster state DQIS: Alice's measurement and the (unnormalized) state obtained by Bob and Rex. Ket $|0 + 0\rangle$ represents the 3-qubit state $|0\rangle|+\rangle|0\rangle$, and so on.

Bob's measurement	State obtained
$ 00\rangle$	$\alpha +\rangle + \beta -\rangle$
$ 01\rangle$	$\alpha -\rangle + \beta +\rangle$
$ 10\rangle$	$\alpha +\rangle - \beta -\rangle$
$ 11\rangle$	$\beta +\rangle - \alpha -\rangle$

TABLE II: 4-qubit cluster state DQIS (type 1): Bob's measurement and state obtained by Rex.

C. Example: DQIS with a QEC code space

Quantum error correcting (QEC) codes [49, 50] are n -qubit graph states up to local transformations. A QEC code word is stabilized by $n - k$ independent stabilizer operators, where k is the code rate.

Let $|G_0\rangle$ and $|G_1\rangle$ be respectively, the 5-qubit 1-bit error correcting code words introduced by Bennett et al. [51]:

$$\begin{aligned} |0_L\rangle &= \frac{1}{4}(-|00000\rangle - |11000\rangle - |01100\rangle - |00110\rangle - |00011\rangle - |10001\rangle + |10010\rangle + |10100\rangle + |01001\rangle \\ &\quad + |01010\rangle + |00101\rangle + |11110\rangle + |11101\rangle + |11011\rangle + |10111\rangle + |01111\rangle) \\ |1_L\rangle &= XXXXX|G_0\rangle, \end{aligned} \quad (14)$$

where $XXXXX$ signifies an application of X on each qubit. We let Alice have qubit 1, Bob qubits 2 and 3, Charlie qubit 4, while recoverer Rex have qubit 5. We let $|G_0\rangle = |O_L\rangle$ and $|G_1\rangle = |1_L\rangle$ in Eq. (6). Alice teleports state $|0\rangle$ by measuring in the Bell basis an ancillary qubit prepared in that state, and her part of the entanglement $|\Psi_L\rangle$ in Eq. (6). Bob and Charlie measure in the computational basis. It may be verified that this

choice satisfies the teleportation divergence condition for the choice of **C**. Alice's, Bob's, Charlie's and recoverer Rex's measurement data are tabulated below in Tables III and IV. Rex recovers the secret based on Alice's 1 bit, Bob's 2 bit and Charlie's 1 bit classical communication. Charlie measures his qubit in the computational basis $\{|0\rangle, |1\rangle\}$ while Rex applies the necessary operation to obtain the qubit.

III. NONLOCAL SUBSPACES

We call two or more n -qubit elements $|G_j\rangle$ of a subset \mathcal{D} of the graph state basis as degenerate graph states

with respect to a Hermitian operator P , if

$$P|G_j\rangle = e|G_j\rangle \forall j \in \mathcal{D}, \quad (15)$$

Alice's measurement	State obtained
$ \Phi^\pm\rangle$	$\alpha(- 0000\rangle - 1100\rangle - 0110\rangle - 0011\rangle + 1001\rangle + 1010\rangle + 0101\rangle + 1111\rangle)$ $+ \beta(- 0111\rangle - 1110\rangle + 1101\rangle + 1011\rangle + 0001\rangle + 0010\rangle + 0100\rangle + 1000\rangle)$
$ \Psi^\pm\rangle$	$\alpha(- 1000\rangle - 0001\rangle + 0010\rangle + 0100\rangle + 1110\rangle + 1101\rangle + 1011\rangle + 0111\rangle)$ $+ \beta(0110\rangle - 1111\rangle - 0011\rangle - 1001\rangle - 1100\rangle + 0101\rangle + 1010\rangle + 0000\rangle)$

TABLE III: Alice's measurement and state obtained by Bob, Charlie and Rex in case of teleportation using the Bennett et al. 5-qubit code (14).

Bob's measurement	State obtained
$ 00\rangle$	$\alpha(- 00\rangle - 11\rangle) + \beta(01\rangle + 10\rangle)$
$ 11\rangle$	$\alpha(- 00\rangle + 11\rangle) + \beta(01\rangle - 10\rangle)$
$ 01\rangle$	$\alpha(01\rangle - 10\rangle) + \beta(00\rangle - 11\rangle)$
$ 10\rangle$	$\alpha(01\rangle + 10\rangle) + \beta(00\rangle + 11\rangle)$

TABLE IV: Bob's measurement and state obtained by rest

where e is a real number. If P is the Bell operator \mathcal{B} in Eq. (7), then the states in \mathcal{D} are called Bell-degenerate, and the space spanned by the operators in \mathcal{D} as Bell-degenerate graph subspace.

The set of all local-realist (LR) models for a given number of settings of Alice, Bob et al. is a polytope in a space of correlations. Equations of the kind (7) correspond to its facets [52, 53]. Greenberger, Horne and Zeilinger (GHZ) first showed how entangled states with perfect correlation lead to a dramatic contradiction with LR models [54]. Mermin [41] pointed out how these perfect correlations can be used to construct a Bell-type inequality of the form Eq. (7). The problem of deriving Bell-type inequalities for various kinds of graph states has been explored by different authors in a number of directions [31–41].

We denote by the DQIS *code basis* \mathcal{C} , the set of graph basis elements $|G_j\rangle$ in Eq. (6). Our aim is to construct a Bell operator with respect to which all and only elements of \mathcal{C} are degenerate. Furthermore, they should each violate the corresponding Bell inequality to its algebraic maximum of m , thereby making \mathcal{C} maximally nonlocal. This Bell operator will thus serve as a witness for the nonlocality of the encoded state. We present two complementary approaches to this problem, discussed in the following two subsections.

A. Bell-degeneracy through unresolvability of generators

Suppose that all n generators g_j of a given n -qubit graph basis are involved in the m operators h_k 's that appear in the Bell inequality (7). At most n of them can be independent. If fewer than n are independent, this gives rise to other graph basis state(s) $|G'\rangle$ than $|G\rangle$ that are consistent with $\langle \mathcal{B} \rangle = m$, and thus serves as a basis for degeneracy.

Theorem 1 *Given an n -qubit graph state $|G\rangle$ that maximally violates a Bell inequality Eq. (7), where \mathcal{B} is a non-trivial functional of all n g_j 's, if the number of independent operators h_j in \mathcal{B} is r ($\leq n$), then the dimension of the Bell-degenerate subspace containing $|G\rangle$ is 2^{n-r} .*

Proof. The maximal violation of the Bell inequality (7) by $|G\rangle$ implies that this state satisfies the m constraints $\forall_{j=1}^m h_j \rightarrow +1$. If $r = n$, then one can solve for the g_j 's to obtain a unique solution, which must be $\forall_{j=1}^n g_j = +1$, corresponding to $|G\rangle$. If $r < n$, then there are fewer constraints than variables (n). Since the g_j are two-valued (± 1), this corresponds to 2^{n-r} possible g_j -assignments consistent with the m constraints. ■

If fewer than n generators appear in \mathcal{B} , then there will be additional degeneracy, by virtue of Theorem 2 below. Let Ξ denote the set of Bell-degenerate graph basis states. If the code rate of a DQIS protocol is k bits, we must choose 2^k elements from Ξ that satisfy the conditions (8) and (9). A necessary condition for this is, clearly, $r + k \leq n$.

An example: The linear cluster state $|\phi_{0000}\rangle$ in Eq. (5) is a graph state corresponding to the stabilizing operators $g_1 = XZII \rightarrow +1$, $g_2 \equiv ZXZI \rightarrow +1$, $g_3 \equiv IZXZ \rightarrow +1$ and $g_4 \equiv IIZX \rightarrow +1$. The Bell operator

$$\begin{aligned} \mathcal{B}_1^\phi &= h_1 + h_2 + h_3 + h_4 \\ &= g_1g_3 + g_2g_3 + g_1g_3g_4 + g_2g_3g_4 \\ &= XIXZ + XIYY + ZYYZ - ZYXY, \end{aligned} \quad (16)$$

for which $q = 3$ (at most only 3 terms in Eq. (16) can be simultaneously made positive when assigned determinate values ± 1 non-contextually), so that the local-realist bound is 2. It attains the algebraically maximum value of $m = 4$ when applied to $|\phi_{0000}\rangle$ [32]. The product of any three of the four summands in Eq. (16) is equal to the remaining one, implying that the 4 constraints $\forall_j h_j \rightarrow +1$ imposed by these operators are not independent; only 3 are. By Theorem 1, this corresponds to a Bell-degenerate subspace of dimension 2. Solving for the g_j 's we find $g_4 = h_1h_2 = h_3h_4 \rightarrow +1$. The remaining three generators cannot be resolved, but are subject to the condition $g_1g_2 = h_1h_3 \rightarrow +1$, $g_2g_3 = h_1h_2h_3 \rightarrow +1$, which is consistent with $g_1 = g_2 = g_3 = -1$, apart from of course $g_1 = g_2 = g_3 = +1$. Thus, we find that Ξ additionally contains the state with the *graph signature*

$(-1, -1, -1, 1)$, which corresponds to the state

$$\begin{aligned} |\phi_{110}\rangle &= Z_1 Z_2 Z_3 |\phi_{0000}\rangle \\ &= \frac{1}{2} (|0-0\rangle + |0+1\rangle - |+1+0\rangle - |+1-1\rangle), \end{aligned} \quad (17)$$

which also yields $\langle \mathcal{B} \rangle = 4$. A teleportation configuration under which these two elements of Ξ are teleportation-divergent is thus suitable for secure DQIS.

Suppose l stabilizer generators f_j appear in all the h_j 's in Eq. (7). If $|G\rangle$ is a state that maximally violates Eq. (7), then the $l-1$ constraints imposed by the above requirement correspond to $\sum_{j=0; j \text{ even}}^l C_j = 2^{l-1}$ states obtained by flipping the sign of an even number of these generators, since they preserve the value assignment $f_1 f_2 \cdots f_l \rightarrow +1$, and hence the value assignments $h_j \rightarrow +1$ on these states. For the Bell operator

$$\begin{aligned} \mathcal{B}_2^\phi &= g_2 g_4 (1 + g_1) (1 + g_3) \\ &= ZXIX + YYIX + YXXY - ZYXY, \end{aligned} \quad (18)$$

which also has the local-realist bound of 2, and the same quantum bound of 4 on the state $|\phi_{0000}\rangle$ [31]. Only three of the four summands in the rhs of Eq. (16) are independent, so that by Theorem 1, the dimension of the Bell-degenerate subspace 2, which is immediately seen to correspond to the state obtained by flipping the sign of both g_2 and g_4 : i.e., the state with the graph signature $(1, -1, 1, -1)$, which corresponds to the 4-qubit cluster state $|\phi_{0101}\rangle$ of Section II B.

B. Bell-degeneracy via a stabilized subspace

The other method is applicable to (n, k) graph codes, the subspace of a n -qubit states, stabilized by $n-k$ stabilizer generators g_j , with $k > 0$. We denote by \mathcal{P} the set of these generators. Let us denote by $\mathcal{S}|_{\mathcal{P}}$, the restriction of \mathcal{S} to products of elements in \mathcal{P} . Up to local transformations, QEC codes are graph codes.

Theorem 2 *Given a (n, k) graph code \mathcal{G} stabilized by operators g_j ($1 \leq j \leq n-k$), any Bell operator $\mathcal{B}_{\mathcal{P}}$ of the type (7), obtained by adding only elements $h_j \in \mathcal{S}|_{\mathcal{P}}$ induces a Bell-degenerate subspace of dimension $\geq 2^k$. If $n-k$ of these h_j 's are independent, then the dimension is exactly 2^k .*

Proof. For each of the 2^k graph basis state $|G'\rangle$ stabilized by g_j 's in \mathcal{P} , clearly $h_j \rightarrow +1$ for summands in $\mathcal{B}_{\mathcal{P}}$, implying that the Bell inequality is maximally violated for any state in the subspace spanned by these basis states. If the number of independent stabilizers in $\mathcal{B}_{\mathcal{P}}$ is $r \leq n-k$, then by virtue of Theorem 1, the dimension of the degenerate subspace is $2^k \times 2^{(n-k)-r} = 2^{n-r}$. Setting $r = n-k$ in the last expression above, we obtain 2^k , as desired. \blacksquare

QECC code states are graph states, that satisfy the graph conditions (2) up to local transformations. A set of four stabilizer operators (which need not have the error correcting property for our purpose) for the above 5-qubit code (14) are:

$$\begin{aligned} g_1 &= XYXXI \\ g_2 &= IXYYX \\ g_3 &= ZYIYZ \\ g_4 &= XYZYX. \end{aligned} \quad (19)$$

from which we can construct the following stabilizers, which we cast in the form of a GHZ contradiction with local realism:

$$\begin{aligned} h_1 &\equiv g_1 g_3 g_4 = ZYXXY \rightarrow +1 \\ h_2 &\equiv g_1 g_4 = -IIXZX \rightarrow -1 \\ h_3 &\equiv g_2 g_3 = ZZYIY \rightarrow +1 \\ h_4 &\equiv g_1 g_2 = XZIZX \rightarrow +1 \\ h_5 &\equiv g_1 = XYYXI \rightarrow +1. \end{aligned} \quad (20)$$

This constitutes a GHZ contradiction [54] with any local-realist assignment of definite values to X, Y, Z as can be as follows: in the operators h_j , a Pauli operator always appears twice along a vertical column, implying that the product of the h_j 's should be 1. Yet the product of the above value assignments to the state $|G\rangle$ is -1 . This logical contradiction means that the X, Y, Z 's of the particles cannot be thought of as possessing determinate values independent of the measurement context (the choice of settings on the other particles).

From Eq. (20) one can write down the Bell operator

$$\mathcal{B}_{5q} = h_1 + h_2 + h_3 + h_4 + h_5, \quad (21a)$$

$$= g_1 g_4 (g_3 + 1) + g_2 (g_3 + g_1) + g_1. \quad (21b)$$

Eq. (21b) satisfies the Bell inequality

$$\langle \mathcal{B}_{5q} \rangle \leq 3, \quad (22)$$

as can be seen by evaluating \mathcal{B}_{5q} for all possible 2^5 value assignments ± 1 to X, Y, Z 's in Eq. (21a). By virtue of Theorem 2, both the states $|0_L\rangle$ and $|1_L\rangle$ of (14) as well as any superposition thereof, violate the above inequality maximally, by the value 5. There is no further degeneracy, since four of the h_j 's in Eq. (20) are independent. Solving for the g_j 's we obtain: $g_1 = h_5$; $g_2 = h_4 h_5$; $g_3 = h_3 h_4 h_5$ and $g_4 = h_2 h_5$.

Here are two examples where both the above two theorems must be invoked. The stabilizers for the Steane [50] code are $g_1 = X_4 X_5 X_6 X_7$, $g_2 = X_2 X_3 X_6 X_7$, $g_3 = X_1 X_3 X_5 X_7$, $g_4 = Z_4 Z_5 Z_6 Z_7$, $g_5 = Z_2 Z_3 Z_6 Z_7$ and $g_6 = Z_1 Z_3 Z_5 Z_7$, with a Bell inequality taking the form

$$\begin{aligned} \langle \mathcal{B}_{\text{Steane}} \rangle &= \langle h_1 + h_2 + h_3 + h_4 + h_5 + h_6 \rangle \\ &= \langle g_1 g_2 (g_4 + g_4 g_5 + 1) + g_3 g_5 (g_2 + g_1) + g_5 \rangle \\ &\leq 4, \end{aligned} \quad (23)$$

where $h_1 \equiv g_1 g_2 g_4$, $h_2 \equiv g_1 g_2 g_4 g_5$, $h_3 \equiv g_1 g_2$, and so on sequentially. The quantum mechanical case yields the maximal $\langle \mathcal{B} \rangle = 6$ (the number of h_j 's in Eq. (23)) for any state $\alpha|0_L\rangle + \beta|1_L\rangle$ in the code space of the Steane code. In this case $\mathcal{P} = \{g_1, g_2, g_3, g_4, g_5\}$ implying that all $2^{7-5} = 4$ 7-qubit basis states stabilized by these 5 operators span a Bell-degenerate subspace.

In addition, only 4 of the h_j 's are independent in Eq. (23), in that the following two constraints $h_1 h_2 = h_6$ and $h_4 h_5 = h_3$ appear. Thus for any value assignment of g_6 and g_7 , there are $2^{5-4} = 2$ graph basis states that maximally violate Eq. (23), which are determined by solving for the 5 g_j 's in terms of the 6 operators h_j 's. Solving, we find $g_4 = h_2 h_3 h_6 \rightarrow +1$ and $g_5 = h_6 \rightarrow +1$, while $g_1 g_2 = h_4 \rightarrow +1$, $g_1 g_3 = h_3 h_5 \rightarrow +1$ and $g_2 g_3 = h_2 h_5 \rightarrow +1$. This corresponds to the graph signatures $(1, 1, 1, 1, 1)$ and $(-1, -1, -1, 1, 1)$ in the first five g_j 's. Thus in all there is Bell-degeneracy of $4 \times 2 = 8$.

The stabilizers for the Shor code [55] are $g_1 = ZZIIIIII, g_2 = IZZIIIIII, g_3 = IIIIZZIII, g_4 = IIIIZZIII, g_5 = IIIIZZZI, g_6 = IIIIZIZZ, g_7 = XXXXXXIII, g_8 = IIIXXXXXX$ for which a Bell inequality takes the form

$$\begin{aligned} \langle \mathcal{B}_{\text{Shor}} \rangle &\equiv \langle h_1 + h_2 + h_3 + h_4 + h_5 + h_6 + h_7 \rangle \\ &= \langle g_3 g_8 (g_1 g_4 + g_5 g_7 + g_2 + g_7) + g_8 (g_4 g_5 + 1) \\ &\quad + g_1 g_2 \rangle \leq 5, \end{aligned} \quad (24)$$

where $h_1 \equiv g_3 g_8 g_1 g_4$, $h_2 \equiv g_3 g_8 g_5 g_7$, $h_3 \equiv g_3 g_8 g_2$, and so on, sequentially. while the quantum mechanical state yields $\langle \mathcal{B} \rangle = 7$ for any state $\alpha|0_L\rangle + \beta|1_L\rangle$ in the code space of the Shor code. In this case $\mathcal{P} = \{g_1, g_2, g_3, g_4, g_5, g_7, g_8\}$ implying that all four 9-qubit basis states stabilized by these 7 operators span a Bell-degenerate subspace.

In addition, only 6 of the 7 h_j 's are independent in Eq. (23), giving rise to 2 degenerate sets in \mathcal{P} . Thus for any of four value assignments to g_6, g_9 , there are two graph basis states that maximally violate Eq. (24), which are determined by solving for the 7 g_j 's in \mathcal{P} in terms of the h_j 's. This yields $g_4 = h_1 h_3 h_7 \rightarrow +1$, $g_5 = h_1 h_3 h_5 h_6 h_7 \rightarrow +1$ and $g_8 = h_6 \rightarrow +1$, while $g_1 g_3 = h_1 h_2 h_4 h_5 \rightarrow +1$, $g_2 g_3 = h_3 h_7 \rightarrow +1$, $g_1 g_2 = h_6 \rightarrow +1$ and $g_3 g_7 = h_4 h_7 \rightarrow +1$. This corresponds to the graph signatures $(1, 1, 1, 1, 1, 1, 1)$ and $(-1, -1, -1, +1, +1, -1, +1)$ for the g_j 's in \mathcal{P} . Thus, in all, we obtain Bell-degeneracy of $4 \times 2 = 8$.

IV. SECURITY CONSIDERATION: TOWARDS A DEVICE-INDEPENDENT SCENARIO

Although the security of quantum key distribution (QKD), has been known for some time, recent work has uncovered the close connection between security (that legitimate participants can distil secret bits) and the violation of a Bell inequality, both in the two-party as well as multi-party [45, 46] scenarios, an intuition that already exists in the Ekert protocol [44].

This connection has assumed further importance for other reasons: a proof of security based on the violation of Bell type inequality is expected to hold good in any nonlocal, non-signaling theory [47], and even in a device independent scenario [48], i.e., one where there is a lack of complete characterization of devices used. The eavesdropper may be the vendor from whom Alice and Bob purchase their (entangled) states and devices. Eve may insert hidden dimensions into the devices, and unknown correlations into the states, that would empower side channels that leak to her information about Alice's and Bob's measurement choices and outcomes.

Thus a conventional check of error rates will not do. The legitimate parties must verify that the correlation data has not been produced by a separable state in a larger dimensional space [56]. However, if the legitimate parties verify via simultaneous local operations and classical communication that a Bell inequality is violated to a sufficiently high level, then, assuming no-signaling, the correlations are guaranteed to allow distillable secrecy [57, 58]. This is a consequence of the monogamy [59] of quantum correlations and holds good in nonlocal, non-signaling theories [60], though no-signaling is not necessary [61].

Let us consider the 4-qubit cluster state DQIS considered in Section II B applied to the protocol described earlier in Section II. Alice holds qubit 1, Bob 2 and 3, and, finally, Rex qubit 4 of N copies of the encoded version of the state $|\Psi\rangle$ or one of its encrypted versions. Alice randomly announces the serial number of one of these copies. On each of the remaining $N-1$ copies, Alice randomly makes a measurement drawn from the set $S_A = \{Y, Z\}$, Bob from the set $S_B = \{XI, YI, XX, YX\}$, and Rex from $S_R = \{X, Y\}$. They classically communicate their measurements and outcomes to Alice. About $4/(2 \times 4 \times 2) = 1/4$ of these are found to have measured one of the four 4-qubit observables appearing as a summand in \mathcal{B}_2^ϕ in Eq. (18), and the parties verify that the outcomes are consistent with the sufficiently high violation of the Bell inequality $\langle \mathcal{B}_2^\phi \rangle \leq 2$. Importantly, by prior synchronization of clocks, each participant must measure her or his observable simultaneously, in order to avoid the possibility of a signaling from the source to the measurement apparatuses [62]. Bounding the timing of the classical communication is used to ensure this.

Conditioned on their passing the Bell test, they proceed to implement the DQIS protocol to allow Rex to reconstruct the state $|\Psi\rangle$. If not, then they may either abort the run of the protocol, and restart from a fresh distribution of entangled states.

As an illustration of the role of monogamy, we consider below a simple single-qubit attack by Eve on a DQIS protocol based on the 5-qubit state (14), which produces a lowering of the violation of the Bell inequality observed by Alice, Bob, and Rex. This is because an attempt by Eve to extract information entangles her system with theirs, causing the latter to diffuse from the code space $\text{span}\{|G_0\rangle, |G_1\rangle\}$. It is important that the degeneracy is

restricted to the code space, since otherwise diffusion of the state to degenerate non-coding sectors would not be detected by looking for a reduction in the Bell inequality violation.

In the device independent scenario, Eve's hidden dimensions will become entangled with the the legitimate particles, thereby producing a detectable dip in the observed maximal violation of the Bell inequality (22). Thus sufficiently high violation of this inequality guarantees that the entangled state lies within the code space, and is uncorrelated with unknown degrees of freedom.

Suppose Eve attacks the fourth qubit of an encoded

state in the span of the codewords (14), via a 1-qubit attack given by the interaction:

$$U(\theta) = \frac{1+Z}{2} \otimes \mathbb{I} + \frac{1-Z}{2} \otimes \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}, \quad (25)$$

which continuously varies from an identity operation to CNOT as θ ranges in $[0, \pi/2]$.

Applying U on the encoded state and her ancilla prepared in the state $|0\rangle$, Eve transforms an arbitrary logical state as:

$$\begin{aligned} (\alpha|0_L\rangle + \beta|1_L\rangle)|0\rangle &\longrightarrow |\Psi\rangle_{ABCDE} \\ &= \frac{1}{\sqrt{2}} ([\alpha|0_L;0\rangle + \beta|1_L;0\rangle] |0\rangle_E + [\alpha|0_L;1\rangle + \beta|1_L;1\rangle] (C|0\rangle + S|1\rangle)), \end{aligned} \quad (26)$$

where $|j_L; k\rangle$ denotes the superposition of terms in the above 5-qubit code word encoding bit j having bit k in the fourth position; C and S denote $\cos(\theta)$ and $\sin(\theta)$,

$$\begin{aligned} \rho_{ABCD} &= \frac{1}{2} (([\alpha|0_L;0\rangle + \beta|1_L;0\rangle] + C[\alpha|0_L;1\rangle + \beta|1_L;1\rangle]) ([\alpha\langle 0_L;0| + \beta\langle 1_L;0|] + C[\alpha\langle 0_L;1| + \beta\langle 1_L;1|]) \\ &+ S^2 (\alpha|0_L;1\rangle + \beta|1_L;1\rangle) (\alpha\langle 0_L;1| + \beta\langle 1_L;1|)), \end{aligned} \quad (27)$$

which has support in the 4-dimension Hilbert space spanned by $\{|0_L;0\rangle, |0_L;1\rangle, |1_L;0\rangle, |1_L;1\rangle\}$.

Since $h_m|j_L\rangle = |j_L\rangle$, it follows that either $h_m|j_L; k\rangle$ equals $|j_L; k\rangle$ or $|j_L; \bar{k}\rangle$. In particular, from Eq. (19), it follows that the action of the h_m 's is to leave $|j; k\rangle$ invariant or to toggle it in the second index (when there is a X or Y in the 4th index). Thus:

$$h_m|j_L; k\rangle = \begin{cases} |j_L; k\rangle & (m = 1, 2, 5) \\ |j_L; \bar{k}\rangle, & (m = 3, 4) \end{cases} \quad (28)$$

One then finds that

$$\text{Tr}_E(h_m \rho_{ABCD}) = \begin{cases} \text{Tr}_E(\rho_{ABCDE}) = \pm 1 & (m = 2, 3, 4) \\ -\cos(\theta) & (m = 1, 5), \end{cases} \quad (29)$$

from which it follows that

$$\langle \mathcal{B}_{5q} \rangle = 3 + 2 \cos(\theta), \quad (30)$$

implying that the attack can be witnessed by a reduction in the degree of violation of the Bell inequality (22), dropping all the way down the local-realistic bound of 3

respectively. The reduced density operator for state with the legitimate agents is given by:

when the attack is maximal with $\theta = \pi/2$. It should be noted in the general case, the tolerable Bell inequality violation will be well above the local-realistic bound.

V. CONCLUSIONS

The protocol of DQIS, which inverts the role of the input state and channel, will be useful in situations where the dealer has bounded quantum memory, and cannot stock secrets but is able simply prepare a fixed state when transmission is needed. Classical encryption can be used to protect the encoded state if required. The coding graph states must possess suitable teleportation divergence properties for DQIS to work, and must be Bell degenerate for proving security via a Bell test on the encoded state. We studied two methods of producing Bell degeneracy. A simple example of DQIS with a 5-qubit QECC was presented. The use of the nonlocal properties of the code states is a useful way to perform security check, and particularly indispensable in the device independent scenario. Further, a proof of security is expected to hold good in any non-signaling, nonlocal theory, which

is useful in the unlikely event that quantum mechanics

turns out to be invalid.

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).

[3] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Nature* **390**, 575 (1997).

[4] G. Rigolin, *Phys. Rev. A* **71**, 032303 (2005).

[5] F.-G. Deng, C.-Y. Li, Y.-S. Li, H.-Y. Zhou, and Y. Wang, *Phys. Rev. A* **72**, 022338 (2005).

[6] S. Muralidharan and P. K. Panigrahi, *Phys. Rev. A* **77**, 032321 (2008).

[7] B. Pradhan, P. Agrawal, and A. K. Pati, <http://arxiv.org/abs/0705.1917>.

[8] M.-L. Li, L. Ye, and J. Yang, *Jl. Atomic Molecular Sci.* **3**, 64 (2012).

[9] S.-B. Zheng, *Phys. Rev. A* **74**, 054303 (2006).

[10] S. Muralidharan and P. K. Panigrahi, *Phys. Rev. A* **78**, 062333 (2008).

[11] S. Bandyopadhyay, *Phys. Rev. A* **62**, 012308 (2000).

[12] A. Pathak and A. Banerjee, *International J. Quantum Information* **9**, 389 (2011).

[13] D. Gottesman, *Phys. Rev. A* **61**, 042311 (2000).

[14] M. Hillery, V. Bužek, and A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999).

[15] S.-B. Zheng, *Phys. Rev. A* **74**, 054303 (2006).

[16] A. Karlsson, M. Koashi, and N. Imoto, *Phys. Rev. A* **59**, 162 (1999).

[17] R. Cleve, D. Gottesman, and H.-K. Lo, *Phys. Rev. Lett.* **83**, 648 (1999).

[18] S. K. Singh and R. Srikanth, *Phys. Rev. A* **71**, 012328 (2005).

[19] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou, *Phys. Rev. A* **72**, 044301 (2005).

[20] W. Tittel, H. Zbinden, and N. Gisin, *Phys. Rev. A* **63**, 042301 (2001).

[21] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, *Phys. Rev. Lett.* **98**, 020503 (2007).

[22] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, *Phys. Rev. Lett.* **95**, 230505 (2005).

[23] D. Schlingemann and R. F. Werner, *Phys. Rev. A* **65**, 012308 (2001).

[24] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).

[25] D. Markham and B. C. Sanders, *Physical Review A* **78**, 042309 (2008).

[26] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, *Phys. Rev. A* **82**, 062315 (2010).

[27] A. Mouzali, F. Merazka, and D. Markham, *Commun. Theor. Phys.* **58**, 661 (2012).

[28] N. Kiesel, C. Schmid, U. Weber, G. Tóth, O. Gühne, R. Ursin, and H. Weinfurter, *Phys. Rev. Lett.* **95**, 210502 (2005).

[29] C.-Y. Lu, X.-Q. Zhou, O. Guehne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan, *Nature Physics* **3**, 91 (2007).

[30] M. Hein, W. Dür, and H.-J. Briegel, *Phys. Rev. A* **71**, 032350 (2005).

[31] O. Gühne and A. Cabello, *Phys. Rev. A* **77**, 032108 (2008).

[32] V. Scarani, A. Acín, E. Schenck, and M. Aspelmeyer, *Phys. Rev. A* **71**, 042325 (2005).

[33] O. Gühne and A. Cabello, *Phys. Rev. A* **77**, 032108 (2008).

[34] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, *Phys. Rev. Lett.* **95**, 120405 (2005).

[35] A. Cabello, *Phys. Rev. Lett.* **95**, 210401 (2005).

[36] G. Tóth, O. Gühne, and H. J. Briegel, *Phys. Rev. A* **73**, 022303 (2006).

[37] A. Cabello, O. Gühne, and D. Rodríguez, *Phys. Rev. A* **77**, 062106 (2008).

[38] D. P. DiVincenzo and A. Peres, *Phys. Rev. A* **55**, 4089 (1997).

[39] L.-Y. Hsu, *Phys. Rev. A* **73**, 042308 (2006).

[40] M. Ardehali, *Phys. Rev. A* **46**, 5375 (1992).

[41] N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).

[42] J. S. Bell, *Rev. Mod. Phys.* **38**, 447 (1966).

[43] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).

[44] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).

[45] V. Scarani and N. Gisin, *Phys. Rev. Lett.* **87**, 117901 (2001).

[46] V. Scarani and N. Gisin, *Phys. Rev. A* **65**, 012311 (2001).

[47] J. Barrett, L. Hardy, and A. Kent, *Phys. Rev. Lett.* **95**, 010503 (2005).

[48] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007).

[49] A. R. Calderbank and P. W. Shor, *Phys. Rev. A* **54**, 1098 (1996).

[50] A. M. Steane, *Phys. Rev. A* **54**, 4741 (1996).

[51] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).

[52] A. Peres, *Found. Phys.* **29**, 589 (1999).

[53] A. Fine, *Phys. Rev. Lett.* **48**, 291 (1982).

[54] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), pp. 69–72.

[55] P. W. Shor, *Phys. Rev. A* **52**, R2493 (1995).

[56] S. Pironio, A. Acín, N. Brunner, N. Gisin, and S. Massar, *New Journal of Physics* **11**, 045021 (2009).

[57] A. Acín, N. Gisin, and L. Masanes, *Phys. Rev. Lett.* **97**, 120405 (2006).

[58] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, *Phys. Rev. A* **74**, 042339 (2006).

[59] V. Coffman, J. Kundu, and W. K. Wootters, *Phys. Rev. A* **61**, 052306 (2000).

[60] L. Masanes, A. Acín, and N. Gisin, *Phys. Rev. A* **73**, 012112 (2006).

[61] M. Pawłowski, *Phys. Rev. A* **82**, 032313 (2010).

[62] E. Hänggi, Ph.D. thesis, ETH Zurich (2010).